EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://versia.com	Checks	9 pruebas
Dominio	versia.com	Hallazgos	50 totales
Fecha	26 de mayo de 2026 a las 09:44	Problemas	16 detectados

D

53/100

puntos de seguridad

RESUMEN EJECUTIVO

El analisis de ciberseguridad realizado sobre el activo digital muestra una puntuacion de 53/100, lo que equivale a una calificacion de grado D. Durante la evaluacion se ejecutaron 9 checks pasivos, de los cuales 4 resultaron exitosos, 2 generaron advertencias y 3 fueron categorizados como fallos criticos. El sitio presenta deficiencias graves en la configuracion de cabeceras de seguridad y mantiene versiones de software obsoletas con vulnerabilidades publicas conocidas. Debido a la combinacion de estos factores, se concluye que el sitio es actualmente vulnerable y requiere intervencion inmediata para mitigar riesgos de explotacion. No se realizo una fase de pentest activo en esta evaluacion.

Resumen de Riesgos

0	7	5	4	34
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	70	AVISO	Certificado expira en 25 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
Deteccion CMS	100	OK	CMS detectado: WordPress, PrestaShop
Version CMS Expuesta	20	FALLO	WordPress 4.9.10 expuesta, WordPress 2.7 expuest...
Seguridad de Cookies	0	FALLO	cookielawinfo-checkbox-necessary: falta HttpOnly...
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 70/100

Estado: AVISO

Certificado expira en 25 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- MEDIO **Dias hasta expiracion**
  25 dias restantes (expira: 2026-06-19T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-05-26T00:00:00.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 0/100

Estado: FALLO

Solo 0/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.2.34 — Revela tecnologia del servidor

- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/7.2.34 — Revela framework/lenguaje
- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- ALTO **X-Frame-Options**
  Falta — Protege contra clickjacking
- ALTO **Strict-Transport-Security**
  Falta — Fuerza conexiones HTTPS (HSTS)
- MEDIO **X-Content-Type-Options**
  Falta — Evita MIME-type sniffing
- MEDIO **Referrer-Policy**
  Falta — Controla la informacion de referer enviada
- MEDIO **Permissions-Policy**
  Falta — Restringe APIs del navegador (camara, micro, etc.)

Redireccion HTTPS — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://versia.com/
- ALTO **HSTS (Strict-Transport-Security)**
  HSTS no configurado — El navegador no fuerza HTTPS
- INFO **Respuesta HTTPS**
  HTTPS responde con status 200

Deteccion CMS — 100/100

Estado: OK

CMS detectado: WordPress, PrestaShop

- INFO **WordPress**
  Detectado via HTML body
- INFO **Joomla**
  No detectado
- INFO **Drupal**
  No detectado
- INFO **Magento**
  No detectado
- INFO **Shopify**
  No detectado
- INFO **PrestaShop**
  Detectado via HTML body
- INFO **Wix**
  No detectado
- INFO **Squarespace**
  No detectado
- BAJO **Meta generator**
  Expone: WordPress 4.9.10
- INFO **Tecnologias detectadas**
  Next.js, PHP/7.2.34

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 4.9.10 expuesta, WordPress 2.7 expuesta

- ALTO **WordPress version**
  Version 4.9.10 expuesta publicamente — Permite a atacantes buscar CVEs conocidos
- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS

- INFO **Archivo /README.txt**
  No accesible (correcto)

Seguridad de Cookies — 0/100

Estado: FALLO

cookielawinfo-checkbox-necessary: falta HttpOnly; cookielawinfo-checkbox-necessary: falta Secure; cookielawinfo-checkbox-necessary: falta SameSite

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- ALTO **Cookie: cookielawinfo-checkbox-necessary — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: cookielawinfo-checkbox-necessary — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: cookielawinfo-checkbox-necessary — SameSite**
  Falta SameSite — Vulnerable a CSRF

Contenido Mixto — 100/100

Estado: OK

No se detecto contenido mixto

- INFO **Contenido mixto**
  Todos los recursos se cargan por HTTPS

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (67 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 1 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **sitemap.xml**
  Presente, ? URLs
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 100/100

Estado: OK

2 puerto(s) abierto(s), todos esperados

- INFO **Puerto 21 (FTP)**
  Cerrado — Transferencia de archivos sin cifrar
- INFO **Puerto 22 (SSH)**
  Cerrado — Acceso remoto seguro
- INFO **Puerto 23 (Telnet)**
  Cerrado — Acceso remoto sin cifrar
- INFO **Puerto 25 (SMTP)**
  Cerrado — Envio de correo
- INFO **Puerto 80 (HTTP)**
  Abierto (esperado) — Servidor web
- INFO **Puerto 443 (HTTPS)**
  Abierto (esperado) — Servidor web seguro
- INFO **Puerto 3306 (MySQL)**
  Cerrado — Base de datos MySQL expuesta
- INFO **Puerto 3389 (RDP)**
  Cerrado — Escritorio remoto Windows
- INFO **Puerto 5432 (PostgreSQL)**
  Cerrado — Base de datos PostgreSQL expuesta

- INFO **Puerto 6379 (Redis)**
  Cerrado — Cache Redis sin autenticacion por defecto
- INFO **Puerto 8080 (HTTP-Alt)**
  Cerrado — Servidor web alternativo / proxy
- INFO **Puerto 27017 (MongoDB)**
  Cerrado — Base de datos MongoDB expuesta

Analisis de Seguridad

VULNERABILIDADES DETECTADAS

[HIGH] WordPress version: La version 4.9.10 detectada esta totalmente obsoleta y permite a atacantes explotar multiples CVEs conocidos para comprometer el sitio.
[HIGH] Content-Security-Policy: La ausencia de esta cabecera facilita la ejecucion de ataques de Cross-Site Scripting (XSS) e inyeccion de contenido malicioso.
[HIGH] X-Frame-Options: La falta de esta configuracion deja el sitio desprotegido frente a ataques de clickjacking que pueden engañar a los usuarios.
[HIGH] Strict-Transport-Security: No se ha configurado HSTS, lo que impide que el navegador fuerce conexiones HTTPS y permite ataques de degradacion de seguridad.
[HIGH] Cookie HttpOnly: La cookie cookielawinfo-checkbox-necessary es accesible via scripts, aumentando el riesgo de robo de sesion en caso de una vulnerabilidad XSS.
[HIGH] Cookie Secure: La cookie mencionada carece del flag Secure, lo que significa que puede ser transmitida a traves de conexiones HTTP no cifradas.
[MEDIUM] X-Content-Type-Options: Al faltar esta cabecera, el sitio es vulnerable a ataques de MIME-type sniffing para ejecutar archivos con contenido inesperado.
[MEDIUM] Referrer-Policy: No existe una politica que controle que informacion de referencia se comparte con terceros al navegar por los enlaces.
[MEDIUM] Permissions-Policy: El sitio no restringe el acceso a APIs sensibles del navegador como la camara, el microfono o la geolocalizacion.
[MEDIUM] Cookie SameSite: La ausencia de este atributo en las cookies incrementa la superficie de ataque para ejecuciones de Cross-Site Request Forgery (CSRF).
[MEDIUM] Archivo /readme.html: Este archivo es accesible publicamente y revela informacion tecnica sobre la instalacion del CMS que facilita el reconocimiento externo.
[LOW] SSL/TLS Expiration: El certificado de seguridad caduca en 25 dias, lo que podria provocar la interrupcion del servicio y alertas de seguridad en breve.
[LOW] Server header expuesto: La cabecera revela el uso de Apache/2.4.6 sobre CentOS y OpenSSL/1.0.2k, informacion valiosa para buscar exploits especificos del servidor.
[LOW] X-Powered-By expuesto: Se confirma el uso de PHP/7.2.34, permitiendo a un atacante conocer la tecnologia exacta de ejecucion del lado del servidor.
[LOW] Meta generator: La etiqueta meta expone publicamente el uso de WordPress 4.9.10 en el codigo fuente.
[LOW] Ruta sensible en robots.txt: El archivo incluye una referencia directa al directorio de administracion, orientando a posibles atacantes sobre la estructura interna.